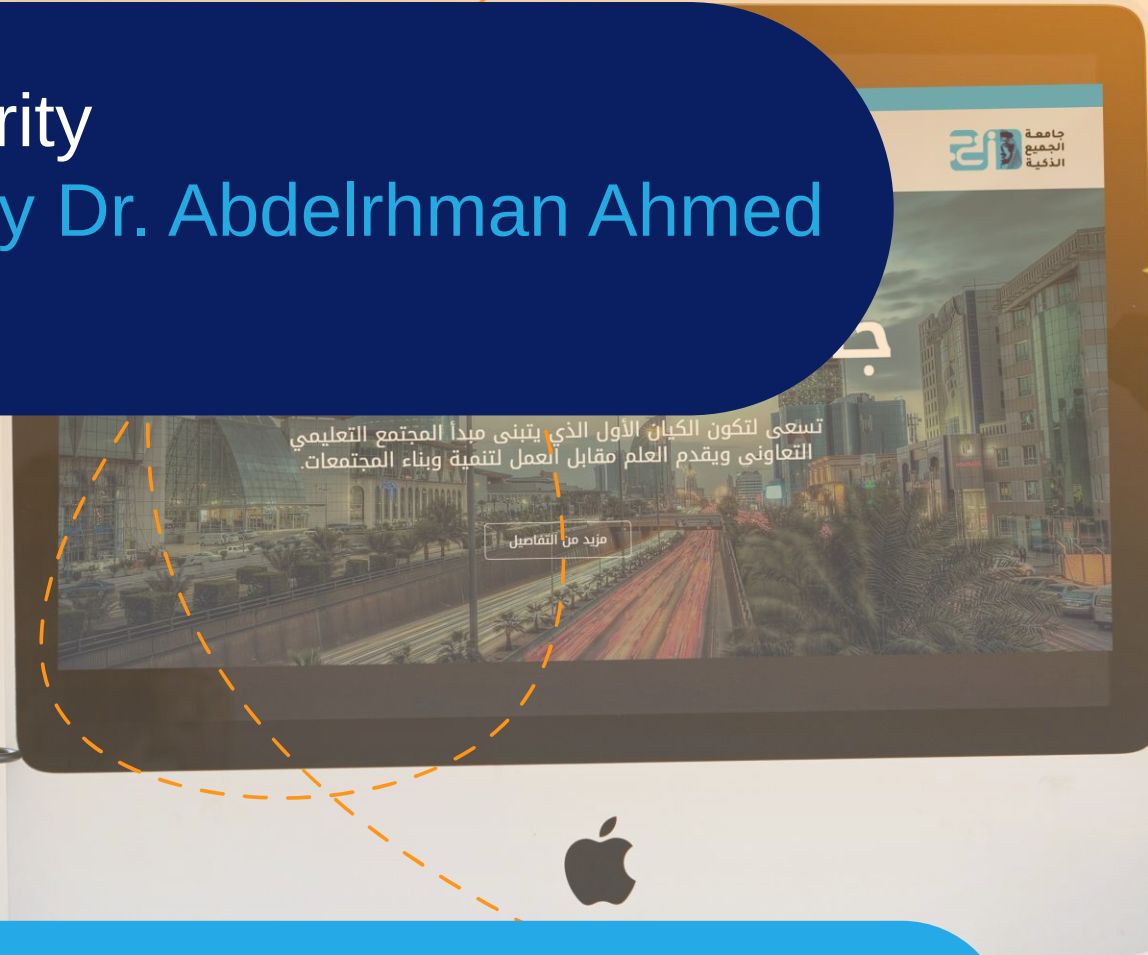


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 3



Device Initial Login



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

VRP Overview

- **Versatile Routing Platform (VRP)**

- ❑ Network operating system
- ❑ Software platform that supports multiple types of devices
- ❑ Provides TCP/IP routing services

- VRP is a network operating system used Huawei routers, Ethernet switches, and service gateways to implement network access and interconnection services. It provides a unified user and management interface, implements control plane functionality, and defines the interface specifications of the forwarding plane (so that the interaction between a product's forwarding plane and the VRP control plane can be implemented). It also implements the network interface layer to shield the differences between the link and network layers of each product.

Introduction to Command Line

- The CLI is divided into command views. All commands must be executed in command views. You can run a command only after you enter its command view.

<NGFW>	User view
<NGFW>system-view	
[NGFW]	System view
[NGFW]interface GigabitEthernet 0/0/1	
[NGFW-GigabitEthernet0/0/1]quit	Interface view
[NGFWJospf 1	
[NGFW-ospf-1]	Protocol view

Introduction to Command Line

- VRP commands use level-defined protection. The four command levels are visit, monitoring, configuration, and management levels.
 - ❑ Visit level: Network diagnosis commands (such as ping and traced) and commands that are used to access external devices from the local device (for example, Telnet client, SSH, and Rlogin). Commands at this level cannot perform file storage configurations.
 - ❑ Monitoring level: Commands at this level are used for system maintenance or service fault diagnosis, including the display and debugging commands. Commands at the monitoring level cannot be saved in configuration files.
 - ❑ Configuration level: Service configuration commands, including routing commands and commands at each network layer, are used to provide direct network services for users.
 - ❑ Management level: Commands at this level affect normal system operation. Such commands include file system, FTP, TFTP, X modem download, configuration file switchover, standby board control, user management, command level setting, and system internal parameter setting commands.
- The system classifies login users into four levels, each of which correspond to a command level. That is, after logging in to the system, a user can use only the commands that are assigned to a level equal to or lower than the user's level. To switch a user from a lower level to a higher level, run the following command: `super password [level user-level] {simple | Cipher} password`.



- Full help displays all the keywords or parameters after you enter a question mark (?) in the command line.
- In any command view, enter ? to obtain all commands and a brief description of each in the command view.

```
<NGFW>?
User view commands:
  anti-ddos      Defend against DDoS attacks
  arp            Specify ARP configuration information
```

- You can also enter a command (if it is a keyword) followed by a space and ? to obtain all keywords and a brief description of each.

```
<NGFW>display firewall ?
  blacklist      Indicate the blacklist command group
  dataplane      Indicate dataplane to manageplane
  defend         Indicate attack defense
```

- Partial help displays all the keywords or parameters that start with the character string entered in the command line.
- ❖ a Type a character string followed by ? to obtain all keywords that begin with the character string

```
<NGFW>d?  
debugging      delete  
dir            display  
download
```

- You can also enter a command followed by a character string and ? to obtain all keywords starting with the character string.

```
<NGFW>display b?  
backup-configuration  bfd  
bgp                  bridge  
buffer               bulk-stat
```

- If there is only one match for an incomplete keyword:

```
[NGFW]info-  
[NGFW]info-center
```

- If there are multiple matches for a keyword:

```
[NGFW]info-center      1  
[NGFW]info-center      lo  
[NGFW]info-center      loghost  
[NGFW]info-center      local  
[NGFW]info-center      logbuffer  
[NGFW]info-center      logfile
```

- Enter an incomplete keyword and press Tab. The system automatically executes partial help:
 - If the match is unique, the system replaces the original input with a complete keyword and displays the keyword on a new line, with the cursor a space behind.
 - If no keyword is matched or multiple keywords are matched, the prefix is displayed first. Press Tab to switch from one matched keyword to another with the cursor placed on the last letter of the keyword. Press the space bar to enter the next word.
 - If you enter an incorrect keyword and press Tab, the keyword is displayed in a new line. The entered keyword does not change.

Configuring Interfaces

- Choose Network > Interface and select the interface to be modified.
- Configure an IP address for the interface and switch the interface mode.

The screenshot shows the 'Modify GigabitEthernet Interface' window. The 'Interface Name' is 'GigabitEthernet1/0/1'. The 'Virtual System' is 'public'. The 'Zone' is 'Select a zone.'. The 'Mode' is 'Routing' (selected), 'Switching', and 'Bypass'. The 'IPv4' tab is active, and 'Static IP' is selected under 'Connection Type'. The 'IP Address' field is empty, with a red box around it and an arrow pointing to a blue box that says 'Configure the IP address and subnet mask.'. The 'Default Gateway', 'Primary DNS Server', and 'Secondary DNS Server' fields are empty. The 'Multi-Egress Options' checkbox is unchecked. The 'Interface Bandwidth' section is at the bottom. There are two blue boxes with red arrows pointing to them: one pointing to the 'Zone' dropdown with the text 'Add to the security zone.', and another pointing to the 'Mode' radio buttons with the text 'Switch the interface mode. The available modes are Routing (Layer 3), Switching (Layer 2), and Hybrid (Layer 2 and 3).'. A red box around the 'IP Address' field has an arrow pointing to a blue box that says 'Configure the IP address and subnet mask.'. The 'IP Address' field has a red box around it and an arrow pointing to a blue box that says 'Configure the IP address and subnet mask.'. The 'IP Address' field has a red box around it and an arrow pointing to a blue box that says 'Configure the IP address and subnet mask.'.

Modify GigabitEthernet Interface

Interface Name: GigabitEthernet1/0/1

Alias:

Virtual System: public

Zone: Select a zone.

Mode: ☒ Routing ☐ Switching ☐ Bypass

IPv4 IPv6

Connection Type: ☒ Static IP ☐ DHCP ☐ PPPoE

IP Address: [Empty field]

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

☐ Multi-Egress Options

Interface Bandwidth:

OK Cancel

Annotations:

- Add to the security zone.
- Switch the interface mode. The available modes are Routing (Layer 3), Switching (Layer 2), and Hybrid (Layer 2 and 3).
- Configure the IP address and subnet mask.

- Configuration procedure:

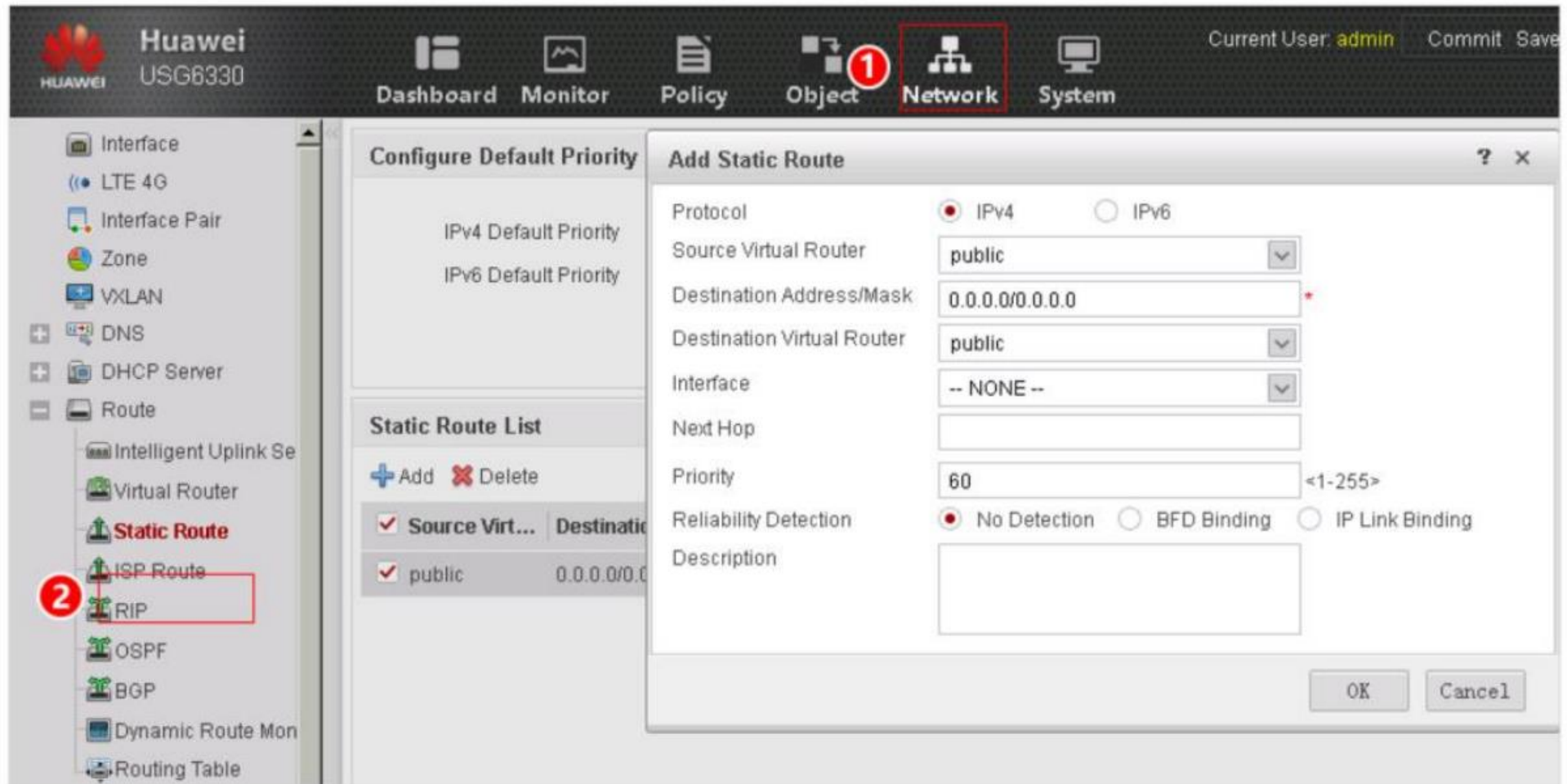
- ☐ Choose Network > Interface and select the interface to be modified.
- ☐ Configure an IP address for the interface and add the interface to the security zone.

- Key commands:

- Enter the view of an interface.
- **<USG>** system-view
- **[USG]** interface interface-type interface-number
- Configure a Layer 3 or Layer 2 Ethernet interface.
- Configure a Layer 3 Ethernet interface.
- Ip address Ip-address { mask | mask-length }
- Configure a Layer 2 Ethernet interface.
- Port switch
- Assign the interface to a security zone.
- Run the system-view command to enter the system view.
- Run the firewall zone [name] zone-name command to create a security zone and enter the view of the security zone.
- Run the add interface interface-type interface-number command to assign the interface to the security zone.



- Choose Network > Route > Static Route and click Add.



- To configure a static route, perform the following operations:

- Run the system-view command to enter the system view.
- Run the ip route-static ip-address { mask | mask-length } {interface-type interface number | next-ip-address } [preference value] [reject | blackhole] command to add a static route.

- To configure the default route, perform the following operations:

- Run the system-view command to enter the system view.
- Run the ip route-static 0.0.0.0 { 0.0.0.0 | 0 } {interface-type interface-number | next- ip-address } [preference value] [reject | blackhole] command to configure the default route.

- You can configure a static route to ensure that traffic sent between two entities always follows this route. However, if the network topology changes or a fault occurs, the static route does not change automatically and requires manual intervention.

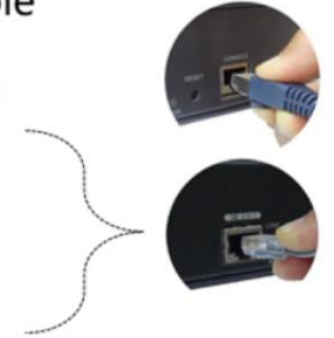
- The default route is used only when no matching access entry is available in the routing table (that is, the routing table does not contain a specific route). The default route is a route to the network 0.0.0.0/0 and is used if the destination IP address of a packet does not match any access entry in the routing table. If no default route exists and the destination IP address of the packet is not in the routing table, the packet is discarded. In this case, an ICMP packet is returned to the source to report that the destination IP address or network is unreachable.

- Device Login Management

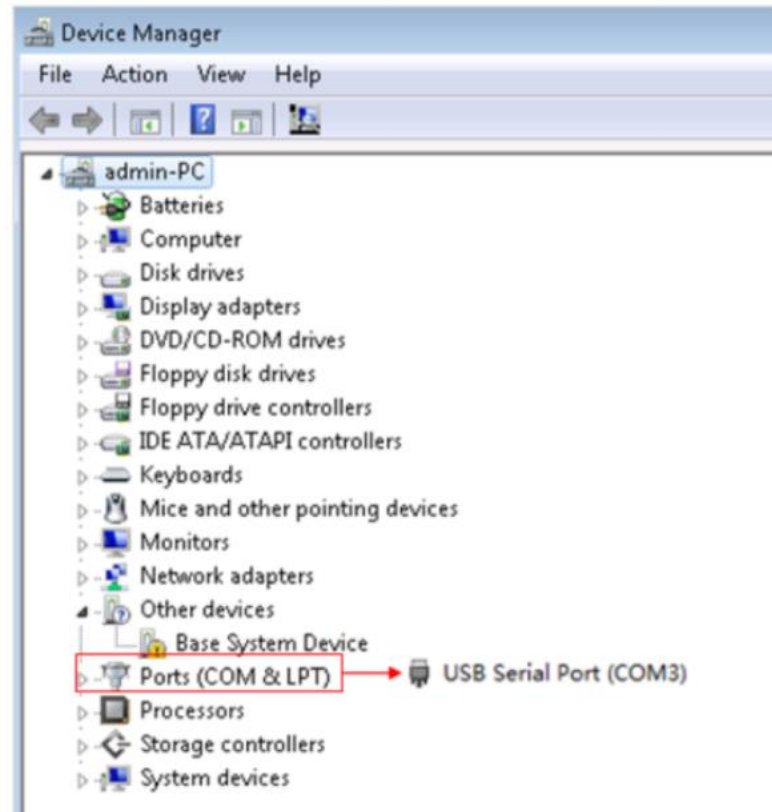
- **Console:** Connect a PC to the console port of a device through an RS-232 serial interface cable. Then, log in to the device through the PC, and configure the device after it is powered on. This login mode is useful if the device cannot be accessed remotely, or the system cannot be started. In the latter case, the console port can be used to diagnose faults or enter the BootROM to upgrade the system.
- **Telnet:** Connect a PC to the device over the network. Then, log in to the device through Telnet to perform local or remote configuration. The device performs user authentication according to the configured login parameters. This login mode enables remote management and maintenance of the device.
- **SSH:** This login mode uses secure transmission channels to enhance security of data exchange. It provides powerful authentication functions to ensure information security and protect devices against attacks, such as IP spoofing attacks.
- **Web:** Access the device through the web browser on a client to control and manage the device.

- Device login management

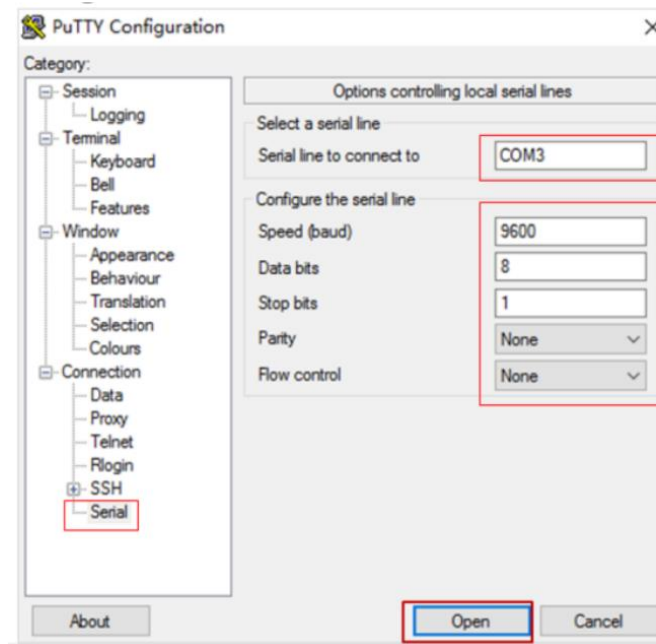
- Console
- Telnet
- SSH
- Web



- Check the parameters of the local port.
- Right-click My Computer, choose Properties from the shortcut menu, and click Device Manager. Check parameters in the Device Manager window.



- Configure the connection interface and communications parameters:
- In the Serial window shown in the figure, set Serial line to connect to based on the port used by the PC (or configuration device), specify PuTTY configuration parameters on the left according to the parameter table on the right, and click Open.
- The default username and password for logging in to the USG configuration interface are admin and Admin@123 respectively. The username is case insensitive, and the password is case sensitive.

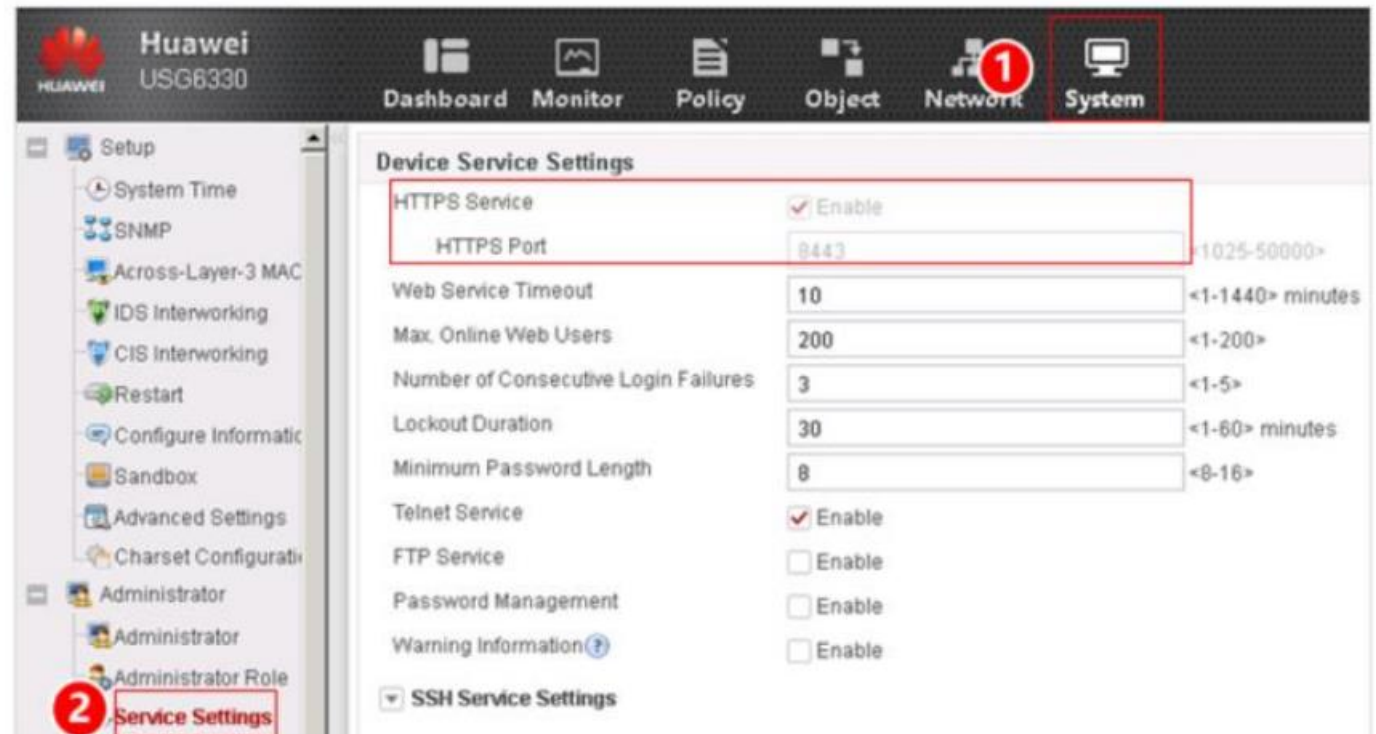


Parameter	Value
Speed (baud)	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

- By default, you can log in to the device through GigabitEthernet O/O/O.
- Set the IP address obtaining mode for network connection to obtain an IP address automatically on the administrator' s PC.
- Directly connect the PC Ethernet interface to the default management interface on the device or connect them through a switch.
- Enter `https://192.168.0.1` in the browser to access the web login page.
- The default username is admin, and its password is Admin@123.
- Configure a PC to obtain an IP address automatically. Connect the PC Ethernet interface to the default management interface on the device directly or through a switch. Enter `https://192.168.0.1` in the PC's web browser to access the web login page.
- The default username and password is admin and Admin@123 respectively.



- If you need to log in to the device through the service interface in web mode, configure the web login function on the device.
- Enable the web management function, enable HTTP or HTTPS management according to requirements, and set the port number
- Enable the web management function:
 - [USG] web-manager security enable interface 8443



➤ Configure a web administrator

• Configure a web user.

- ❑ [USG] aaa
- ❑ [USG-aaa] manager-user webuser
- ❑ [USG-aaa-manager-user-webuser] password cipherAdmin@123
- ❑ [USG-aaa-manager-user-webuser] service-type web
- ❑ [USG-aaa-manager-user-webuser] level 3

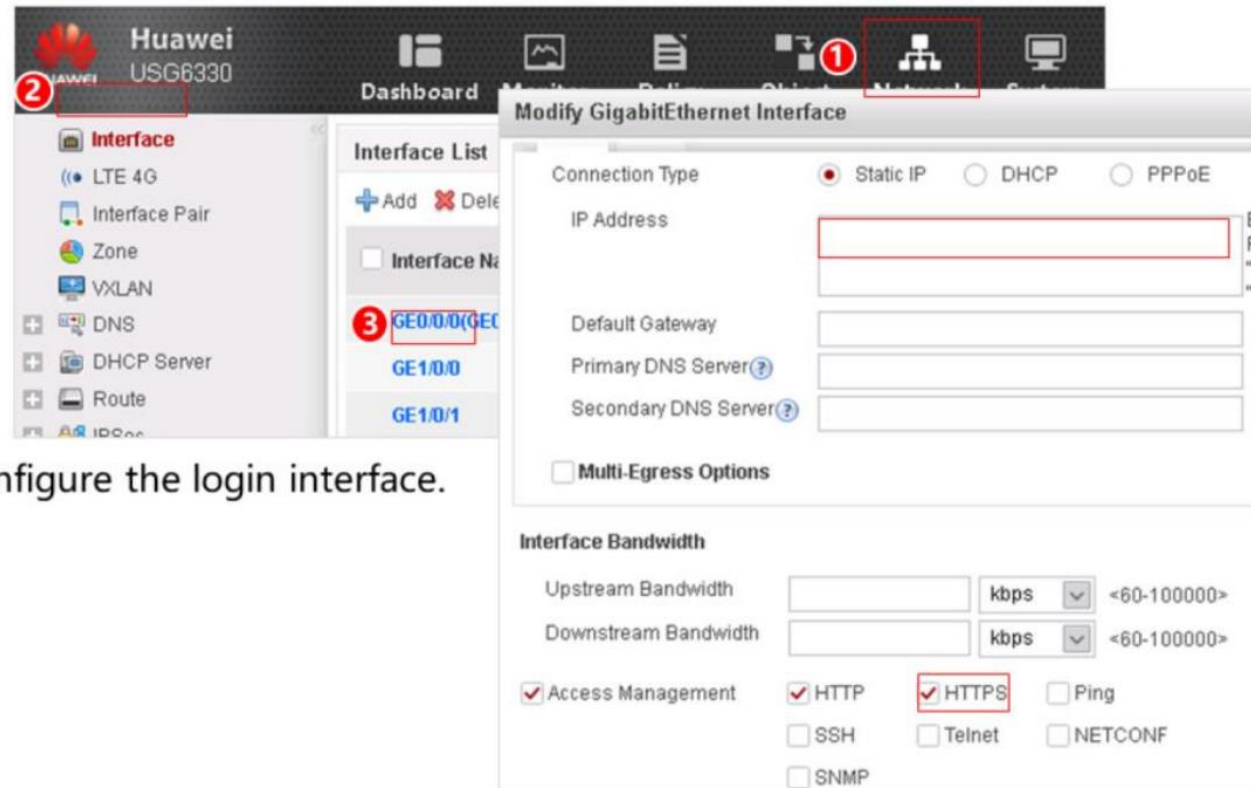
The screenshot displays the Huawei USG6330 web management interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Policy', 'Object', 'Network', and 'System' (highlighted with a red box and number 1). The left sidebar shows 'Setup', 'Administrator', 'Administrator Role', and 'Service Settings', with 'Administrator' highlighted (red box and number 2). The main area shows the 'Administrator List' with an 'Add' button (red box and number 3) and a 'Delete' button. The 'Add Administrator' dialog box is open, showing the following fields:

- Name:** A text input field.
- Authentication Type:** Radio buttons for 'Local authentication' (selected), 'Server authentication', and 'Server authentication/Local authentication'.
- Password:** A text input field with a red box around it. A note below states: "The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. The password cannot contain two or more consecutive identical characters. The password cannot be the same as the administrator name or its reverse form."
- Confirm Password:** A text input field.
- Role:** A dropdown menu.
- Trusted Host 1:** A text input field with a green plus icon.
- Advanced Settings:** A section with 'Service Type' options: 'Web' (checked with a red box), 'Telnet', 'SSH', 'Console', 'FTP', and 'API'.

At the bottom right of the dialog box are 'OK' and 'Cancel' buttons.

- Configure web device management on the USG interface:

- ☐ [USG-GigabitEthernet1/0/1] service-manage enable
- ☐ [USG-GigabitEthernet1/0/1] service-manage https permit



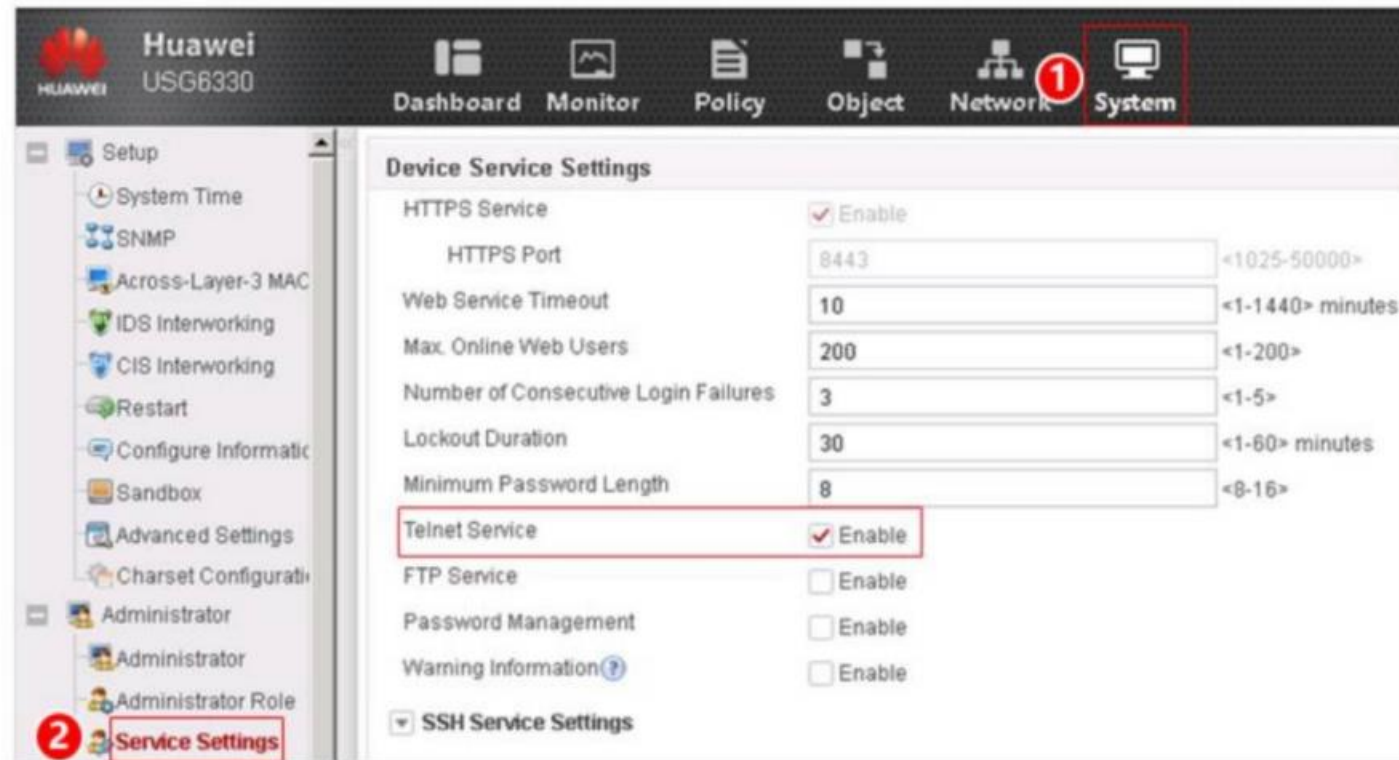
- Configure the login interface.

- By default, Telnet login is disabled on the NGFW. To use Telnet, log in to the NGFW in another mode and enable the Telnet service.

- Enable the Telnet service.

- Enable the Telnet service:

- [USG] telnet server enable



The screenshot shows the Huawei USG6330 web interface. The 'System' menu is highlighted with a red circle 1. The 'Administrator' menu item is highlighted with a red circle 2. The 'Add' button is highlighted with a red circle 3. The 'Add Administrator' dialog box is open, showing the following fields:

- Name: [Empty text box]
- Authentication Type:
 - ☒ Local authentication
 - ☐ Server authentication
 - ☐ Server authentication/Local authentication
- Password: [Empty text box] (8-64 characters)
- Confirm Password: [Empty text box]
- Role: [Empty dropdown menu]
- Trusted Host 1: [Empty text box]
- Advanced Settings:
 - Service Type:
 - ☐ Web
 - ☒ Telnet
 - ☐ SSH
 - ☐ Console
 - ☐ FTP
 - ☐ API

Configure a Telnet administrator.

- Configure the vty interface:

- ☐ [USG] user-interface vty 0 4
- ☐ [USG-ui-vty0-4] authentication-mode aaa

- Configure a Telnet administrator:

- ☐ [USG] aaa
- ☐ [USG-aaa] manager-user vtyadmin
- ☐ [USG-aaa-manager-user-vtyadmin] password
- ☐ Enter Password
- ☐ [USG-aaa-manager-user-vtyadmin]] service-type telnet
- ☐ [USG-aaa-manager-user-vtyadmin]] level 3

- Configure the login interface.
- Configure Telnet device management on the USG interface:
 - ☐ [USG-GigabitEthernet1/0/1] service-manage enable
 - ☐ [USG-GigabitEthernet1/0/1] service-manage telnet permit

Modify GigabitEthernet Interface

IPv4 | IPv6

Connection Type: ☒ Static IP | ☐ DHCP | ☐ PPPoE

IP Address: Enter each IP address on a separate line.
For example:
"1.1.1.1/255.255.255.0"
"1.1.1.1/24".

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

☐ Multi-Egress Options

Interface Bandwidth

Upstream Bandwidth: kbps <60-100000> | Overload Protection Threshold: %

Downstream Bandwidth: kbps <60-100000> | Overload Protection Threshold: %

☒ Access Management

☐ HTTP | ☐ HTTPS | ☒ Ping

☐ SSH | ☒ Telnet | ☐ NETCONF

☐ SNMP

- SSH provides greater security and powerful authentication functions for users to log in to the device. Configure SSH device management on the USG interface. The administrator can enable SSH device management as required.

- Configuration commands:

- Enable the STelnet service.

```
[NGFW]stelnet server enable
```

- Configure SSH management on the USG interface.

```
[NGFW-GigabitEthernet1/0/1]service-manage enable  
[NGFW-GigabitEthernet1/0/1]service-manage ssh permit
```

- Configure a local RSA key pair.

```
<NGFW>system-view  
[NGFW]rsa local-key-pair create
```

- Configure VTY user interfaces.

```
[USG]user-interface vty 0 4  
[USG-ui-vty0-4]protocol inbound all  
[USG-ui-vty0-4]authentication-mode aaa
```

- When the device functions as an SSH server, you can set the authentication mode to Password or RSA for SSH users.
- Create an SSH administrator account and set the authentication mode to Password and service mode to STelnet.

```
[NGFW]aaa
[NGFW-aaa]manager-user sshadmin
[NGFW-aaa-manager-user-sshadmin]service-type ssh
[NGFW-aaa-manager-user-sshadmin]level 3
[NGFW-aaa-manager-user-sshadmin]password cipher huawei
```

- Create an SSH user.

```
[NGFW]ssh user sshadmin
[NGFW]ssh user sshadmin authentication-type password
[NGFW]ssh user sshadmin service-type stelnet
```

- After the preceding configurations are completed, run the SSH client software to establish an SSH connection.
- If a Huawei device functions as an SSH client, enable the SSH login function on the client.

```
[NGFW]ssh client first-time enable
```

- **Device File Management**

- **Configuration file management**
- **System file management (software upgrade)**
- **License management**

- **Overview of Device File Management**

- **The configuration file contains the configurations that the device will load when it is started. You can save configuration files on the device, modify and remove existing configuration files, and specify which configuration file the device will load upon each startup. System files include the USG software version and signature database files. Generally, management of system files is required during software upgrades.**
- **Upgrading system software: The system software can be uploaded to the device through TFTP or FTP. Upgrade the system software to configure the software system for the next startup.**
- **A license is provided by a vendor to authorize the usage scope and validity period of product features. It dynamically controls whether certain features of a product are available.**

- **Configuration file types:**

- ☐ **Saved-configuration:** the configuration file used for the next startup of the USG. It is stored in the flash memory or CF card of the USG and persists across restarts.
- ☐ **Current-configuration:** the configuration currently in use on the USG. It is modified by command lines and web operations. It is stored in the memory of the USG and persists across restarts. Common operations for the configuration file
- ☐ **Save the configuration file.**
- ☐ **Erase the configuration file (restore to factory settings).**
- ☐ **Configure the system software and configuration file for the next startup.**
- ☐ **Restart devices.**

- **Save the configuration file:** Enable the firewall to use the current configuration as the start configuration the next time it restarts.
 - **Method 1 (command line):** Run the save command in the user view.
 - **Method 2 (web):** Click Save in the upper right corner of the home page.
- **Erase the configuration file (restore to factory settings):** After the configuration file is erased, the firewall uses the default parameter settings the next time it restarts.
 - **Method 1 (command line):** Run the reset saved-configuration command in the userview.
 - **Method 2 (web):** Choose System > Maintenance > Configuration Management to restore to factory settings.
 - **Method 3 (hardware reset button):** If the device is not powered on, press and hold the RESET button, and turn on the power switch. When the device indicator blinks twice per second, release the RESET button. The device starts with the default configuration.
 - **Method 4 (hardware reset button):** If the device is started normally, press and hold the RESET button for more than 10 seconds. The device restarts and uses the default configuration.

- **Configure the system software and configuration file for the next startup:**
 - ❑ **Command line:** Run the startup system-software sysfile command in the user view.
 - ❑ **Web:** Choose System > Maintenance > System Update, and then select Next Startup System Software.
- **Restart the firewall:**
 - ❑ **Function:** The firewall will be restarted, and the restart will be recorded in logs.
 - ❑ **Method 1 (command line):** Run the reboot command in the user view.
 - ❑ **Method 2 (web):** Choose System > Maintenance > System Restart.

- One-click upgrade

Current User: admin Commit Save Help About

Dashboard Monitor Policy Object Network **1** System

System Upgrade

Current Version USG6330 V500R001C80SPC100 (VRP (R) software, Version 5.170) Details

System Upgrade File List

Server IP Address: sec.huawei.com [Server Connectivity Test]

File Name	Currently Used File	Startup File	State	Operation
System File	hda1:jusg6000v500r001c80spc100.bin	hda1:jusg6000v500r001c80spc100.bin		3 [One-Click Upgrade] [Select]
Patch File		hda1:jusg6000_v500r001sph012.pat		[One-Click Upgrade] [Select]

System Upgrade **2**

One-Click Version Upgrade ?

1 Preparation

Before upgrading, you are advised to:

- Ensure that the target version is different from the version in use.
- Export the device alarm, log, and configuration information.

Alarm Information Export

Log Information Export

Configuration Export Save

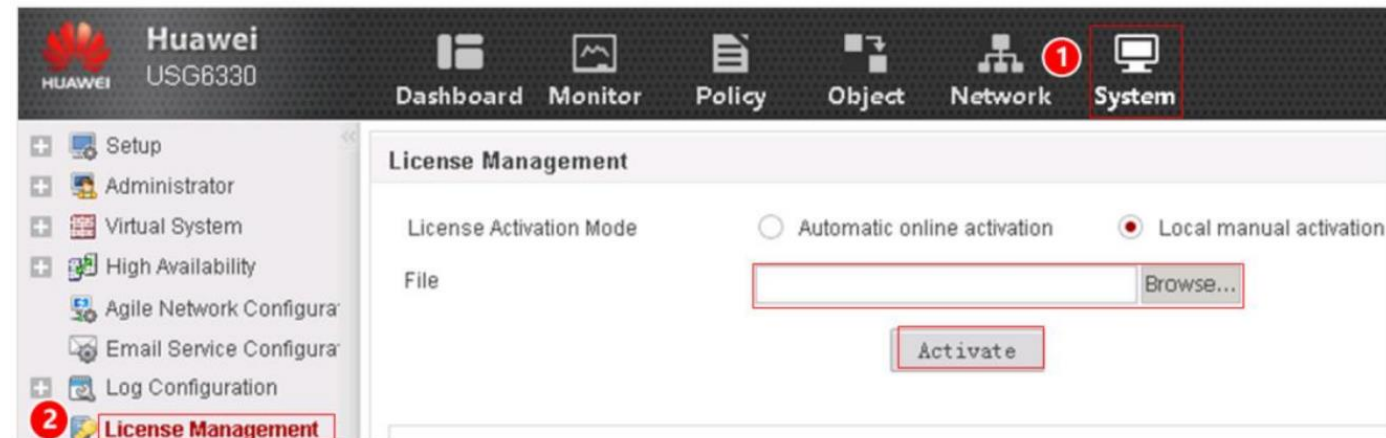
hda1 Total: 1.13 GB Free: 270.7 MB

System Software Browse...

2 Version Upgrade

- **One-click upgrade of the system software:**
 - ❑ If the device has insufficient storage space available, the device automatically deletes the system software that is running.
- **System software files are stored as .bin files.**
 - ❑ Choose System > System Update.
 - ❑ Click One-Click Version Upgrade. The One-Click Version Upgrade wizard is displayed.
 - ❑ Optional: Click the Export button sequentially to export the device's alarm, log, and configuration information to the PC. You are advised to save the configuration information to the terminal.
 - ❑ Click Browse. Select the system software to be uploaded.
 - ❑ If the current network allows the device to restart immediately after upgrade, select either Set as the next startup system software, and restart the system or Set as the next startup system software, and do not restart the system according to requirements.
 - ❑ The upgraded system software can be used only after the device restarts.
 - ❑ Configuration using commands (the FW acts as an FTP client)

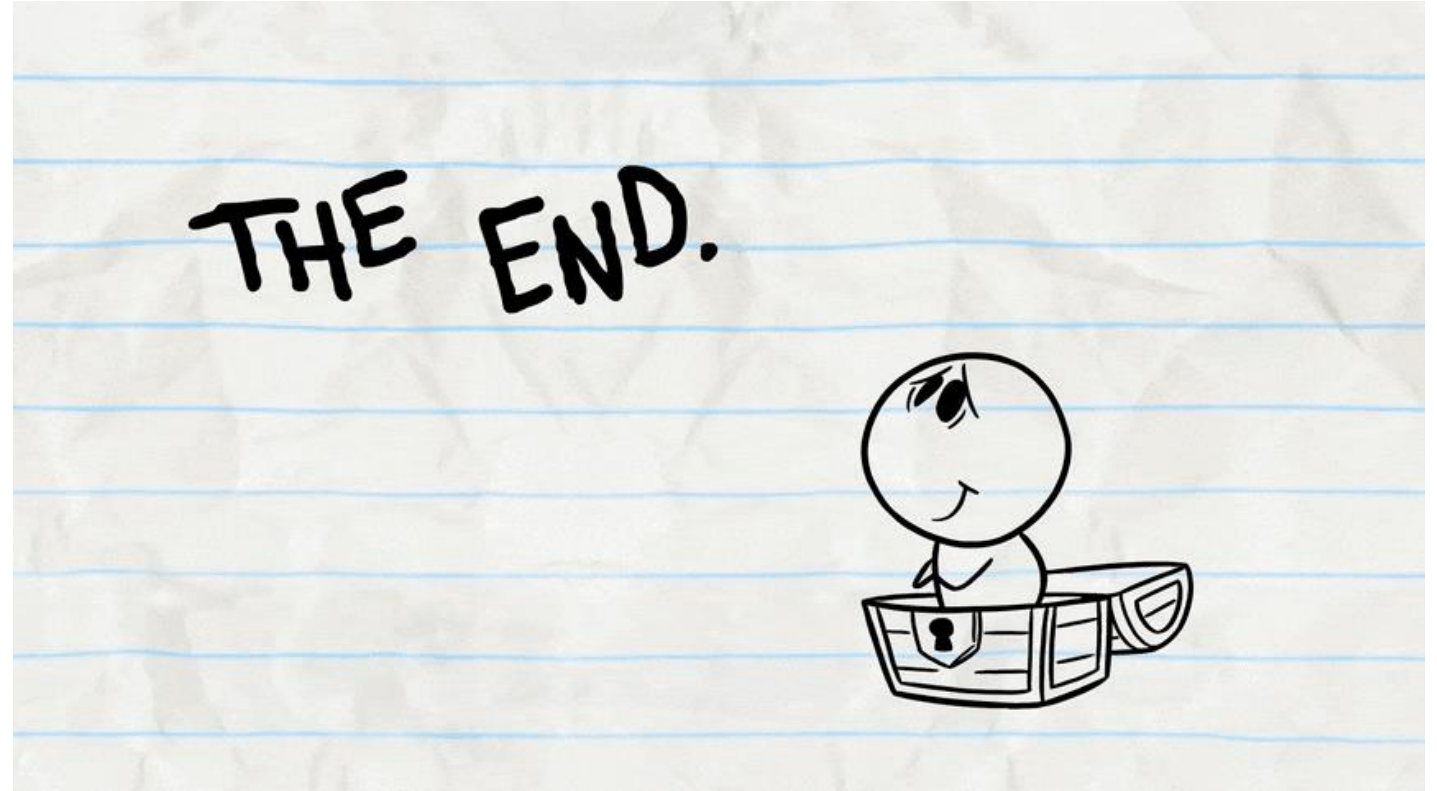
- A license is provided by a vendor to authorize the usage scope and validity period of product features. It dynamically controls whether certain features of a product are available.
- Activate a license.
 - The license can be activated online or offline. You can activate the license automatically through Huawei security center at sdplsp.huawei.com or manually activate it locally.
 - License files are stored as .dat files. The software file name cannot contain any Chinese characters.
 - Configuration commands:
 - ❑ Run the system-view command to enter the system view.
 - ❑ Run the license active license-file command to activate the specified license file.
 - ❑ Run the display license command to view the license information.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY